Cyber Warfare

Hybrid War

โดย พลเอก เอกชัย ศรีวิลาศ

ผู้อำนวยการสำนักสันติวิธีและธรรมาภิบาล

สถาบันพระปกเกล้า

Technology/Innovation

- เทคโนโลยีใหม่ ๆ เกิดขึ้นมากมาย อาทิ Internet of Things, Robots, Artificial Intelligence (AI), Drones, Blockchain, Virtual reality, 3D Printing และ Electric vehicle ซึ่งเข้ามามีบทบาทในโลกมากขึ้น

- หากมองในด้านผู้ใช้งานเทคโนโลยีขั้นพื้นฐานอย่าง Internet พบว่าคนไทยมีอัตราการใช้ Internet ต่อหัวมากกว่าค่าเฉลี่ยโลกและกลุ่มประเทศเอเชียแปซิฟิก และใช้เวลากับ Mobile Internet มากที่สุดในโลก เฉลี่ย 4 ชั่วโมงต่อวัน คนไทยในกรุงเทพมหานครใช้ Facebook มากที่สุดในโลก

คำพูดของ Jack Ma ในการบริหารคน

“**ผมไม่รู้อะไรเกี่ยวกับเทคโนโลยีหรือการจัดการก่อนที่จะเริ่มธุรกิจ**เลยข้อเท็จจริงก็คือ คุณไม่จำเป็นต้องรู้อะไรมากมาย **คุณเพียงแค่ต้องหาคนที่ฉลาดกว่าคุณเองมาร่วมทำงานด้วย** ซึ่งเป็นเวลาหลายปีที่ผมพยายามหาคนที่เก่งกว่าผมเสมอ และเมื่อคุณพบคนเก่งมากมายแล้ว **งานของผมก็คือการทำให้แน่ใจว่าคนฉลาดสามารถทำงานร่วมกันได้**”

(อ้างอิงจาก https://www.youtube.com/watch?v=IhPZfLlouLE)

NEWS

ด่วน!! อีเมล์ ถูกแฮก 773 ล้านบัญชีทั่วโลก เราจะเช็คและป้องกันอย่างไร

By Pantawat — On ม.ค. 18, 2019

Share

อีเมล์ ถูกแฮก มากกว่า 773 ล้านบัญชีทั่วโลก

HOME NEWS CULTURE LIFESTYLE OPINION VIDEO PODCAST MAGAZINE CONTACT

WORLD TECH

พบข้อความส่วนตัวของผู้ใช้ Facebook อย่างน้อย 81,000 บัญชี ถูกแฮกและขายในโลกออนไลน์

โดย คมปกิต สกุลหวง
03.11.2018

3.1K

การโจมตีทางไซเบอร์ที่ซอฟต์แวร์แอนตี้ไวรัส ไม่สามารถป้องกันได้

- ระบบป้องกันความปลอดภัยที่อาศัยซอฟต์แวร์แอนตี้ไวรัส (Anti-Virus) ได้พัฒนาถึงที่สุดแล้ว อย่างที่ Brian Dye อดีต SVP ฝ่ายการจัดการความปลอดภัยข้อมูลของ Symantec ซึ่งเป็นบริษัทยักษ์ใหญ่ของผู้จำหน่ายซอฟต์แวร์ความปลอดภัย
- Dye บอกว่า ซอฟต์แวร์แอนตี้ไวรัส (Anti-Virus) ได้สิ้นสุดลงแล้ว เพราะซอฟต์แวร์แอนตี้ไวรัส (Anti-Virus) ตรวจพบการโจมตีทางไซเบอร์ได้เพียง 45% ที่เหลืออีก55% ไม่สามารถตรวจพบได้
- การพัฒนาระบบป้องกันความปลอดภัยในอนาคต จะต้องศึกษาอย่างเร่งด่วน เพื่อคาดการณ์การโจมตีจากไวรัสคอมพิวเตอร์หรือซอฟต์แวร์หรือรหัสคำสั่งที่ไม่พึงประสงค์อื่นๆ เพื่อป้องกันการเกิดความเสียหายด้วยการโจมตีทางไซเบอร์ที่รุนแรงยิ่งขึ้น
- ปัญญาประดิษฐ์ (AI) จะกลายเป็นที่นิยมในการป้องกันความปลอดภัย

https://www.fujitsu.com/th/th/about/resources/featurestories/whitepaper10.html

Jack Ma พูดถึงเรื่องความปลอดภัยกับ AI

Jack Ma: รู้หรือไม่ว่า แต่ละวันมีคนโจมตีอาลีบาบาทางไซเบอร์กว่า 3 ล้านครั้ง แต่เราให้ AI ซึ่งย่อมาจาก Alibaba Intelligence มาจัดการ

"ผมมักจะบอกกับคนที่คอยป้องกันเหตุร้ายทางไซเบอร์ว่า คนเราถ้าจะรักใครสักคน มันไม่มีเหตุผลหรอก แต่เวลาเราเกลียดใครสักคน เราหาเหตุผลร้อยแปดเพื่อเกลียดคนนั้นให้ได้ ฉะนั้น **ถ้าอยากให้ AI จัดการกับภัยคุกคามทางไซเบอร์ เราก็สอนให้ AI รู้จักและจับพฤติกรรมที่เป็นภัยต่ออาลีบาบาแค่นั้นเอง**"

ปรากฏการณ์ของโลกในศตวรรษที่ 21

- สับสน อลหม่าน (Disorder)
- สลับซับซ้อน (Complexity)
- แข่งขันสูง (High Competition)
- พยากรณ์ไม่ได้ (Unpredictable)
- รวดเร็ว (Speed)
- เกี่ยวโยงกัน (Concerned)
- เครือข่าย (Network)

โลกวันนี้

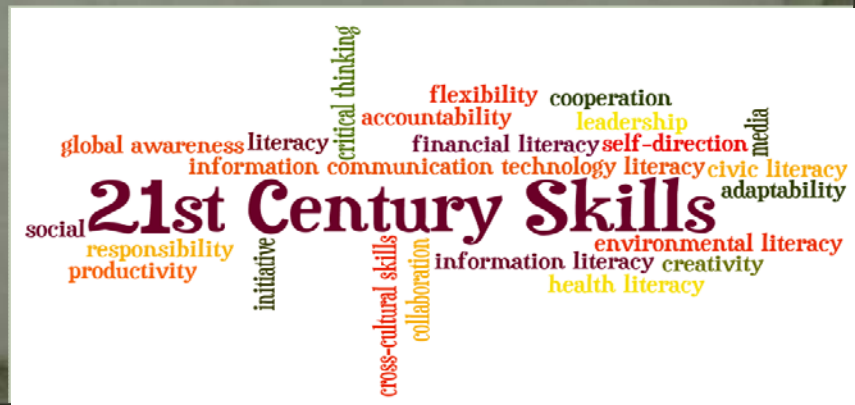
- โลกเรากำลังถูก Disrupt ด้วย 3 กระแสหลัก คือ กระแสโลกาภิวัตน์ กระแสการพัฒนาเทคโนโลยี และกระแสความเป็นใหญ่ของเงินทุน
- เงินเคยเป็นตัวเปลี่ยนอารยธรรมของมนุษย์ โลกาภิวัตน์และเทคโนโลยีทางการเงิน วันนี้เงินกลับมาเป็นตัวขับเคลื่อนโลกในด้านต่าง ๆ อย่างมาก
- อดีตเราต้องทำงานเพื่อแลกเงิน ปัจจุบันเงินสามารถสร้างเงินได้โดยไม่ต้องสร้างมูลค่าจริงทางเศรษฐกิจเลย แถมยังเคลื่อนย้ายได้อย่างรวดเร็ว ซึ่งเงินจะค่อย ๆ พัฒนารูปแบบเป็น Digital มากขึ้น และคนรวยคนจนจะยิ่งมีช่องว่างมากขึ้น
- 3 กระแสหลักนี้ ได้สร้างปรากฏการณ์ทางเศรษฐกิจและสังคมในโลกสมัยใหม่ที่เรียกว่า ‘VUCA’
  - V: volatility = ความผันผวน รวดเร็วรุนแรง
  - U: uncertainty = ความไม่แน่นอน คาดเดาไม่ได้
  - C: complexity = ความซับซ้อน เข้าใจยาก
  - A: ambiguity = ความคลุมเคลือ ไม่ชัดเจน

ทักษะในศตวรรษที่ 21

- **ทักษะการเรียนรู้และนวัตกรรม** มีความคิดสร้างสรรค์ ใส่ใจนวัตกรรม มีวิจารณญาณ แก้ปัญหาเป็น สื่อสารดี เต็มใจร่วมมือ
- **ทักษะสารสนเทศ** สื่อ เทคโนโลยี อัพเดตทุกข้อมูล ข่าวสาร รู้เท่าทันสื่อ รอบรู้เทคโนโลยีสารสนเทศ ฉลาดสื่อสาร
- **ทักษะชีวิตและอาชีพ** มีความยืดหยุ่น รู้จักปรับตัว ริเริ่มสิ่งใหม่ ใส่ใจดูแลตัวเอง รู้จักเข้าสังคม เรียนรู้วัฒนธรรม

ความสำคัญของ 4 ทักษะ

- โลกยิ่งเปลี่ยนเร็วเท่าไร = เรายิ่งต้องสร้างทักษะการเรียนรู้ให้เร็วขึ้นโดยการใช้เทคโนโลยีมาช่วย
- โลกยิ่งมีความไม่แน่นอนสูง = เรายิ่งต้องสร้างทักษะการปรับตัวเพื่อรับความผันแปรและความเสี่ยง
- โลกยิ่งมีความซับซ้อนสูง = เรายิ่งต้องมีที่ยืน สร้างจุดแข็งให้กับตัวเอง
- โลกยิ่งมีความไม่ชัดเจนสูง = เรายิ่งต้องสร้างภาวะผู้นำ



สงครามในรูปแบบต่าง ๆ

สงครามผสม (Compound War)

- เป็นสงครามที่มีลักษณะของการเชื่อมโยงทางยุทธศาสตร์ แต่มีการปฏิบัติที่แยกส่วนกันระหว่างกำลังตามแบบ (Regular War) และกำลังนอกแบบ (Irregular War)
- ใช้การประสานสอดคล้องในการปฏิบัติการทางทหารเป็นหลัก การปฏิบัติการทางทหารจะมีการแบ่งแยกเขตความรับผิดชอบหรือพื้นที่ปฏิบัติการกันอย่างชัดเจน

ตัวอย่างของสงครามผสม

- สงครามปฏิวัติของสหรัฐฯ ที่ใช้ทั้งกำลังทหารหลักและกำลังทหารบ้านหรือกำลังประจำถิ่น ในการต่อสู้เพื่อเอกราชจากอังกฤษ
- สงครามเวียดนามที่ฝ่ายเวียดนามเหนือ ได้ใช้การผสมผสานการปฏิบัติทางทหารระหว่าง กองทัพเวียดนามเหนือและเวียดกง

ประเภทของสงคราม

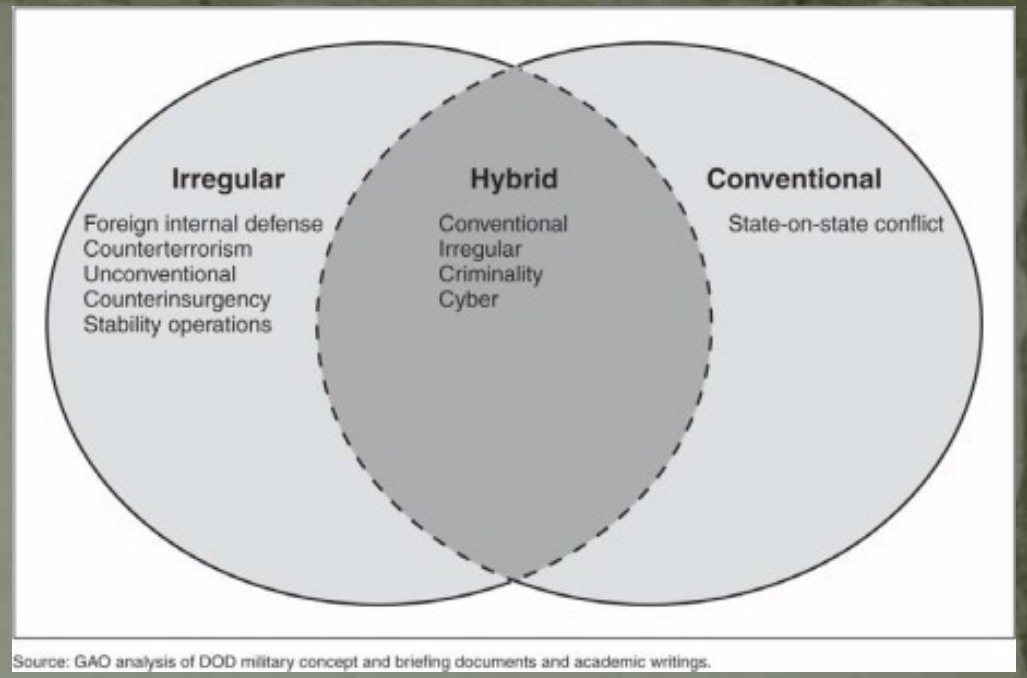
สงครามตามแบบ หรือสมมาตร (Regular Forces)	สงครามนอกแบบ หรืออสมมาตร (Irregular Forces)
1. เป็นการต่อสู้ด้วยกำลังอาวุธ หรือใช้มาตรการทางการทหารเข้าสู้รบกัน	1. เป็นการต่อสู้ด้วยมาตรการต่างๆ ทั้งทางการเมือง เศรษฐกิจ สังคมจิตวิทยา การทูต เทคโนโลยี และการใช้มาตรการทางทหาร
2. เป็นการทำสงครามแบบเปิดเผยตัวตน มีการเผชิญหน้ากันโดยตรงระหว่างกำลังทหารของคู่สงคราม	2. ไม่มีการเผชิญหน้าระหว่างคู่กรณีโดยเปิดเผย
3. เป้าหมายจำกัดที่กำลังทหารเท่านั้น	3. เป้าหมายไม่ได้จำกัดที่กำลังทหารเท่านั้น แต่ยังรวมถึงประชาชนด้วย เป็นสงครามแบบเบ็ดเสร็จ โดยใช้เทคนิคการก่อความไม่สงบและการก่อการร้าย

ประเภทของสงคราม

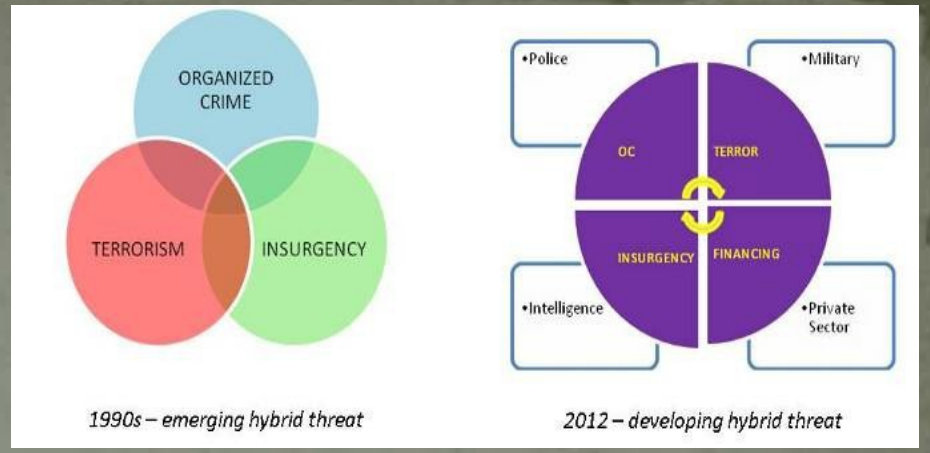
สงครามตามแบบ (Regular Forces)	สงครามนอกแบบ (Irregular Forces)
4. คู่สงครามหรือความขัดแย้งเป็นรัฐต่อรัฐ	4. คู่สงครามหรือความขัดแย้งไม่จำเป็นต้องเป็นรัฐต่อรัฐ แต่จะเป็นรัฐต่อกลุ่มคนที่ไม่ใช่รัฐก็ได้
5. วิธีการดำเนินการแบบพื้นฐาน 3 แบบ คือการยุทธด้วยวิธีรุก ด้วยวิธีรับ และด้วยวิธีร่นถอย รวมถึงการยุทธภายใต้สภาพพิเศษ	5. มีสงครามพิเศษ สงครามการเมือง สงครามนิวเคลียร์ สงครามศาสนา สงครามไซเบอร์ และสงครามประเภทอื่นๆ ที่ไม่สามารถจัดอยู่ในสงครามตามแบบ
6. รวมกำลังเป็นกลุ่มก้อน อันตรายมาก	6. แยกย้ายกระจายกันอยู่ อันตรายน้อย
7. หลักนิยมและยุทธวิธีการรบเป็นระเบียบ ประเมินสถานการณ์ได้ง่าย ข้าศึกทราบหนทางปฏิบัติ และโต้ตอบได้ง่าย	7. ทำการรบไม่มีแบบฉบับ ข้าศึกประมาณสถานการณ์ไม่ถูก ไม่ทราบหนทางปฏิบัติ ตอบได้ยาก

Hybrid War

- Hybrid War เป็นการผสมผสานสงครามหลายรูปแบบ
- ทั้งสงครามตามแบบในระดับต่ำ ปฏิบัติการพิเศษ สงครามไซเบอร์ สงครามอวกาศ และสงครามจิตวิทยา
- ผสมผสานระหว่างขีดความสามารถของสงครามตามแบบ ยุทธวิธีนอกแบบ และการก่อการร้ายที่ใช้ความรุนแรง
- การบีบบังคับขู่เข็นให้เกิดความหวาดกลัว และการก่ออาชญากรรมในรูปแบบต่างๆ



Hybrid War



- เป็นสงครามผสมผสานกำลังตามแบบและกำลังนอกแบบ ปฏิบัติการทางทหารร่วมกันอย่างแยกไม่ออก
- การปฏิบัติการที่มุ่งเป้าหมายไปที่รัฐเสรีประชาธิปไตย และช่องโหว่ของระบบสถาบันผ่านช่องทางต่างๆที่หลากหลาย เช่น การเมือง เศรษฐกิจ ทหาร ประชาชนพลเมือง และข้อมูล...

- สงครามระหว่างอิสราเอล-เลบานอนครั้งที่ 2 (2006)
  - กลุ่มฮิสบุลเลาะห์ เป็นกลุ่มติดอาวุธ ที่ทำสงครามต่อต้านอิสราเอลในเลบานอน เป็นผู้ก่อตั้งต้นแบบของสงครามพันทาง **Hybrid War**

การปฏิบัติการ Hybrid War ของรัสเซีย

"THE RUSSIAN VIEW OF MODERN WARFARE IS BASED ON THE IDEA THAT THE MAIN BATTLESPACE IS THE MIND."
– NATIONAL DEFENCE ACADEMY OF LATVIA POLICY PAPER

- **เป้าหมายหลัก**

1) การยึดดินแดนโดยไม่ต้องใช้กำลังทหารตามแบบอย่างโจ่งแจ้ง ดังเช่น การผนวกดินแดนที่แหลมไครเมียจากยูเครนในปี 2014

2) สร้างเงื่อนไขในการใช้กำลังทางทหารแบบธรรมดาได้ การผนวกดินแดนไครเมียเป็นสัญญาณว่ารัสเซียสามารถใช้ **Hybrid War** แบบนี้เพื่อผนวกดินแดนในที่อื่นได้ เช่น ในกลุ่มประเทศบอลติก

3) ใช้ Hybrid War เพื่อส่งอิทธิพลทางการเมืองและนโยบายต่อประเทศตะวันตกและที่อื่นๆ เป้าหมายเพื่อท้าทายใหญ่ต่อรัฐบาลตะวันตกและสหรัฐ

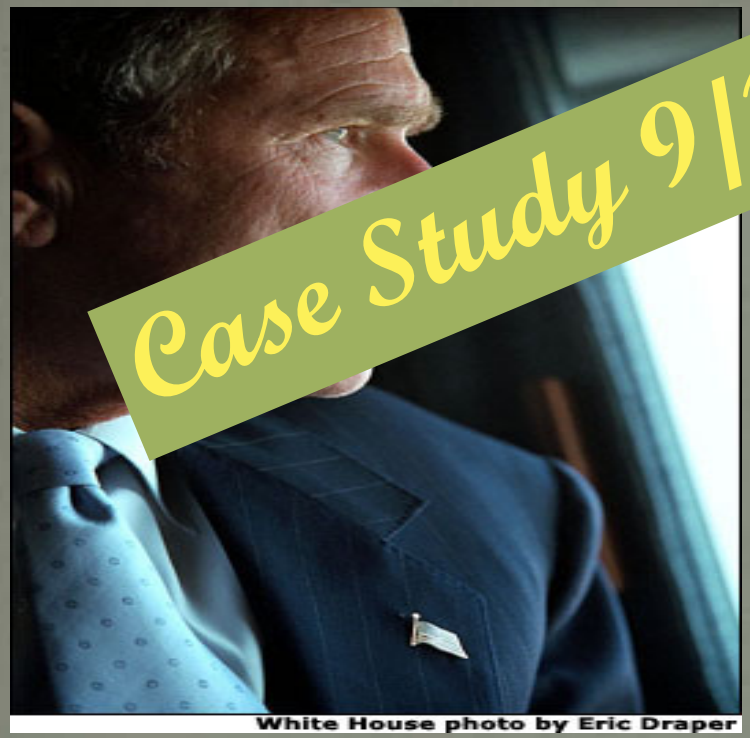
เครื่องมือที่ใช้ใน Hybrid War ของรัสเซีย

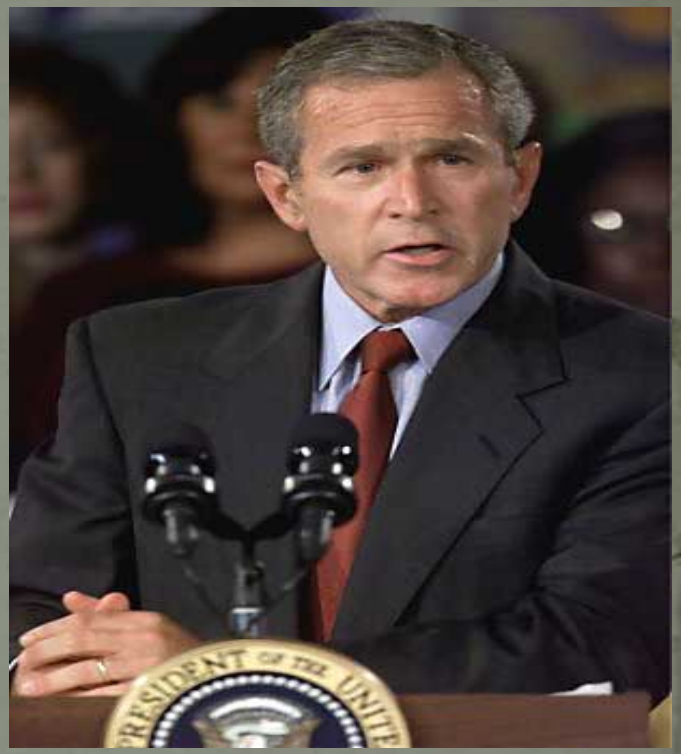
1) **ปฏิบัติการข่าว โดยใช้สื่อ เช่นรัสเซียทูเดย์** เพื่อส่งเสริมทัศนะของรัสเซีย ไปจนถึงการสร้างข่าวปลอม
2) **สงครามไซเบอร์** รัสเซียสร้างนักรบไซเบอร์ขึ้นเป็นจำนวนมากเพื่อล้วงความลับจากระบบข่าวสารตะวันตก
3) **กลุ่มตัวแทนซึ่งมีความเห็นอกเห็นใจในเป้าหมายของรัสเซีย** เช่นกลุ่ม “หมาป่ากลางคืน” ซึ่งเป็นสโมสรนักขับมอเตอร์ไซค์และความบันเทิง
4) **อิทธิพลทางเศรษฐกิจที่สำคัญ** ได้แก่การใช้พลังงานเป็นเครื่องมือทางนโยบายการต่างประเทศ ในหลายประเทศในยุโรปที่ต้องพึ่งพาก๊าซธรรมชาติจากรัสเซียเป็นต้น
5) **มาตรการลับต่างๆ** มีทั้งการติดสินบน การกรรโชก และความพยายามอื่นๆ ในการชักใยนักการเมืองที่มีปัญหาให้สนับสนุนนโยบายของรัสเซีย
6) **อิทธิพลทางการเมือง** ใช้งานทางการทูตธรรมดาๆ เพื่อสนับสนุนบุคคลและพรรคการเมืองที่นิยมหรือเห็นอกเห็นใจรัสเซีย มีการเชิญให้ไปเยือนรัสเซียในฐานะบุคคลสำคัญ

Hybrid War

- การเกิดเหตุก่อวินาศกรรมเมื่อ 9 ก.ย. 2544 หรือ 9/11 ในสหรัฐอเมริกา
  - เป็นการก่อการร้ายที่มีรูปแบบของการปฏิบัติการที่แตกต่างไปจากเดิม ที่มีความรุนแรง และความเสียหายมากขึ้น
  - เป็นขบวนการในทางลับ มีการประสานสอดคล้องอย่างลงตัว และได้สร้างความเสียหายทั้งชีวิต ทรัพย์สินเป็นจำนวนมาก
  - สร้างความหวาดกลัว เสียใจ ความโกรธแค้นให้กับผู้ที่ได้รับผลกระทบโดยตรง ซึ่งส่วนใหญ่ไม่ได้เกี่ยวข้องกับมูลเหตุของความขัดแย้งเพราะเป็นผู้บริสุทธิ์ ที่ถูกเลือกให้เป็นเป้าหมาย

Case Study 9/11 in U.S.A.


White House photo by Eric Draper

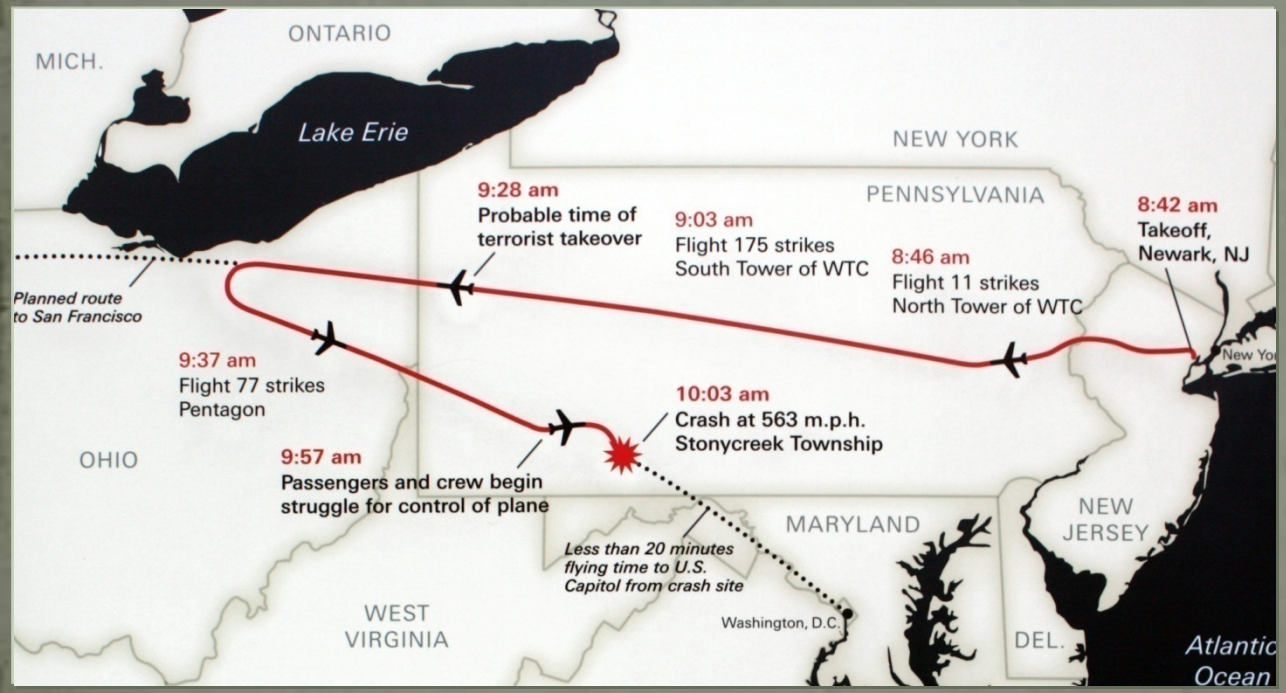


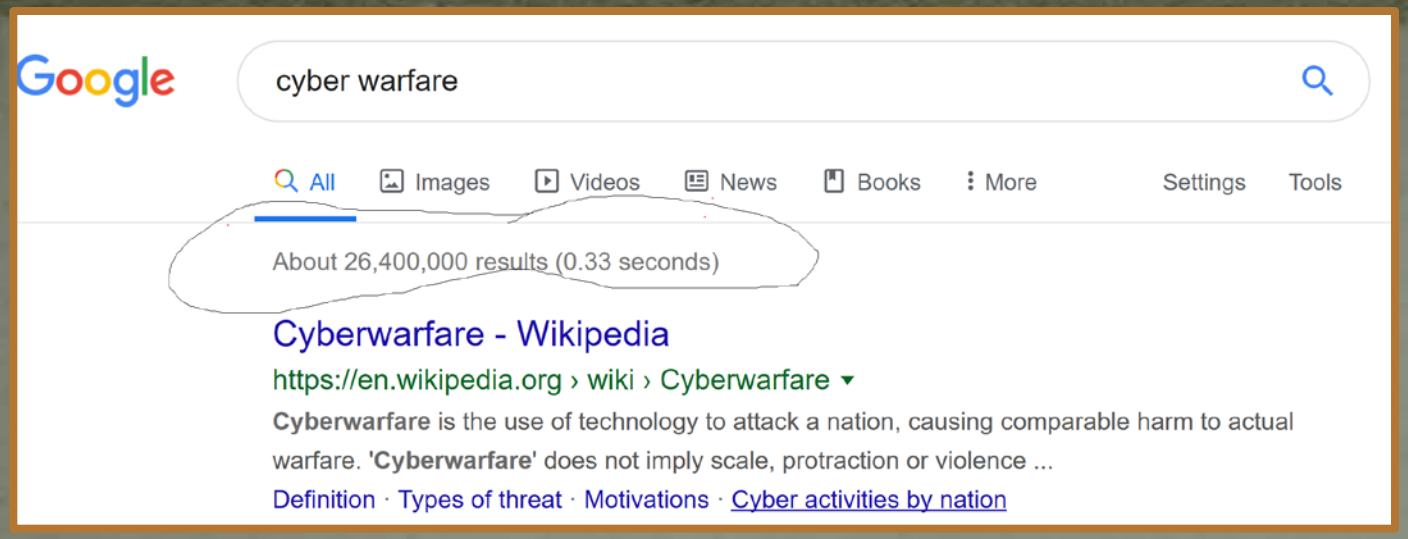
America has stood down enemies before, and we will do so this time.
Bush September, 11, 2001

American Land of Power: Political, Economic and Military

World Trade Building

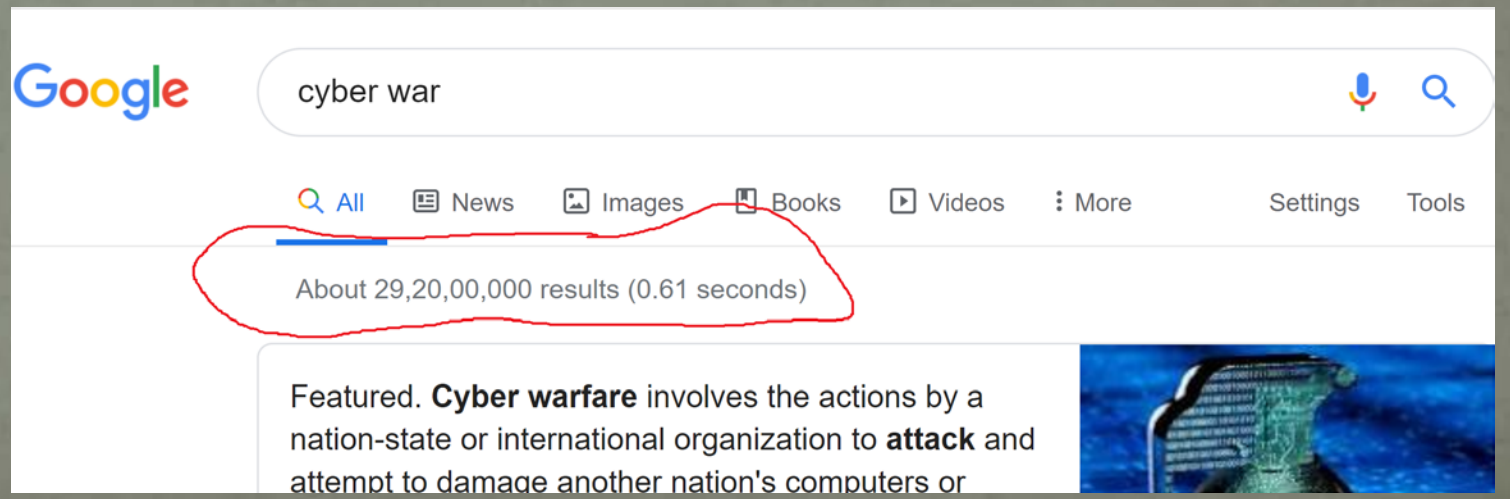
Pentagon building of the
United States Department of Defense


ONTARIO
MICH.
Lake Erie
NEW YORK
PENNSYLVANIA
9:28 am
Probable time of
terrorist takeover
9:03 am
Flight 175 strikes
South Tower of WTC
8:46 am
Flight 11 strikes
North Tower of WTC
8:42 am
Takeoff,
Newark, NJ
Planned route
to San Francisco
9:37 am
Flight 77 strikes
Pentagon
10:03 am
Crash at 563 m.p.h.
Stonycreek Township
OHIO
9:57 am
Passengers and crew begin
struggle for control of plane
MARYLAND
NEW
JERSEY
Less than 20 minutes
flying time to U.S.
Capitol from crash site
WEST
VIRGINIA
Washington, D.C.
DEL.
Atlantic
Ocean



ค้นหาจาก google คำว่า Cyber Warfare พบ 26 ล้าน ข้อความ

Cyber War พบ 29 ล้าน ข้อความ



ภัยคุกคามไซเบอร์

- ภัยคุกคามได้ลุกลามไปทั่วโลก ไม่ว่าจะเป็นการโจมตีระบบธนาคาร 5 แห่งในรัสเซีย
- ข่าวการเจาะระบบการเลือกตั้งของสหรัฐฯ จากแฮ็กเกอร์นอกประเทศ
- แฮ็กเกอร์รัสเซียเจาะระบบ database ของ World Anti-Doping Agency (WADA) องค์กรต่อต้านการใช้สารต้องห้ามโลก และเปิดโปงข้อมูลนักกีฬาสหรัฐฯ
- เหตุการณ์ที่กลุ่ม Anonymous โจมตีออสเตรเลียจนสามารถปิดเว็บไซต์ของหน่วยงานรัฐบาล และรัฐสภา เพื่อประท้วงความพยายามของรัฐบาลออสเตรเลียในการเสนอออกกฎหมายเกี่ยวกับการใช้อินเทอร์เน็ต
- ในทำนองเดียวกันกลุ่ม Anonymous ได้ร่วมกับกลุ่ม Green Party ในการประท้วงการเลือกตั้งในอิหร่าน เป็นต้น

รูปแบบการโจมตีที่เป็น “ภัยคุกคาม” ในปัจจุบัน

1. Malware ความไม่ปกติทางโปรแกรมสูญเสีย C (Confidentiality) I (Integrity) และ A (Availability) อย่างใดอย่างหนึ่ง หรือทั้งหมด สูญเสียความลับทางข้อมูล สูญเสียเสถียรภาพของระบบปฏิบัติการ จะทำลายข้อมูล หรือเข้าควบคุมระบบคอมฯ เคยสร้างความเสียหายให้กับสหรัฐฯ อังกฤษ จีน รัสเซีย สเปน อิตาลี และไต้หวัน มาแล้ว โดยผู้เชี่ยวชาญทางไซเบอร์แจ้งว่ามีการโจมตีด้วยมัลแวร์นี้ถึง 75,000 ครั้งทั่วโลก
2. Phishing “ภัยคุกคาม” เกิดขึ้นเพราะเปิดไฟล์หรือข้อมูลที่มีความเสี่ยง อาชญากรไซเบอร์รู้จึงใช้ระบบ “Phishing” เพื่อจูงใจให้เปิดไฟล์ที่มีมัลแวร์อันตรายแนบไว้ และเมื่อหลงเปิด “มัลแวร์” จะถูกติดตั้งและโจมตีคอมพิวเตอร์ทันที
3. SQL Injection Attack ภาษาโปรแกรมที่ใช้สื่อสารกับฐานข้อมูลภายในเซิร์ฟเวอร์ อาชญากาไซเบอร์จะโจมตีไปที่ SQL ส่งผลต่อเซิร์ฟเวอร์ ที่เก็บ “ข้อมูลของลูกค้า” “ข้อมูลส่วนบุคคล” “ หมายเลขบัตรเครดิตและระบบการเงิน” จะสร้างปัญหาในระยะยาวหากไม่มีการแก้ไขที่ทันท่วงที

รูปแบบการโจมตีที่เป็น “ภัยคุกคาม” ในปัจจุบัน

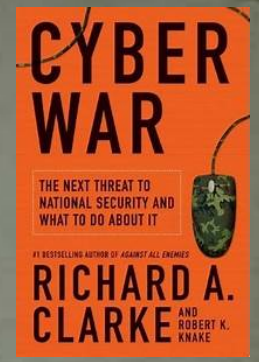
4. Cross-Site Scripting (XSS) โจมตีผ่านเว็บไซต์และเซิร์ฟเวอร์ที่มีช่องโหว่ เพื่อคุกคามฐานข้อมูลต่างๆ โดยเฉพาะข้อมูลด้านการเงิน จะใช้การโจมตีแบบ XSS ที่คล้ายกับการโจมตีแบบ SQL

5. Denial of Service (DoS) โจมตีเหมือนมีคนเข้าเว็บมากเกินไป เกิดความผิดปกติของเซิร์ฟเวอร์หลายๆส่วน พร้อมกันเรียกว่า DDoS หรือ Distributed Denial of Service Attack แก้ไขได้ยากมาก เนื่องจากผู้โจมตีมี IP ที่หลากหลายจากทั่วโลกเข้าสร้างความหนาแน่นของ Traffic บนเซิร์ฟเวอร์

6. Session Hijacking and Man-in-the-Middle Attacks ผู้บุกรุกจะโจมตี Session ด้วยการจับรหัส และวางตัวเองในคอมพิวเตอร์เครื่องที่ร้องขอการใช้งานเสียเอง

7. Credential Reuse การตั้งค่าเข้าสู่ระบบและรหัสผ่าน ช่วยสร้างความปลอดภัยได้ระดับหนึ่ง แต่จะต้องมีรหัสผ่านที่ไม่ซ้ำกันในการเข้าระบบต่างๆ ถ้าตั้งรหัสผ่านไว้แบบเดียวกัน หากโดนขโมยข้อมูลไปจะสร้างความเสียหายครอบคลุมไปในหลายๆส่วน บัญชีหลายๆบัญชีก็จะสามารถถูกแฮ็กได้

สงครามไซเบอร์ ; Cyber war



- **“สงครามไซเบอร์”** เป็นคำนิยามขึ้นมาโดย ริชาร์ด เอ.คลาร์ก ในหนังสือ **“Cyber war”**

(พฤษภาคม 2010) นิยามว่า

“เป็นการกระทำของรัฐ - ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์ หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก”

- การใช้ **“อานุภาพทางไซเบอร์”** ของประเทศใดประเทศหนึ่ง โจมตีประเทศเป้าหมาย เพื่อข่มขู่ คุกคาม หรือทำลายล้าง ประเทศหนึ่งๆ ซึ่งกำลังกลายเป็นภัยคุกคามต่อความมั่นคงในระดับชาติมากขึ้นเรื่อยๆ

สงครามไซเบอร์ Cyber war

- เป็นสงครามที่ไม่ต้องมีการเคลื่อนกำลัง ไม่ต้องมีการยิงปืนใหญ่ ทิ้งระเบิด หรือลั่นกระสุนใดๆ ทั้งสิ้น
- เพียงแค่อยู่หลังคอมพิวเตอร์ก็สามารถจู่โจมระบบการเงิน ระบบสาธารณูปโภค การขนส่ง หรือแม้กระทั้งทำลายระบบการสั่งการทางทหารของประเทศเป้าหมายได้
- จากข่าวการโจมตีธนาคารในหลายแห่งทั่วโลก เช่น ธนาคาร 5 รายใหญ่ในรัสเซียถูกโจมตี เมื่อวันที่ 8 พ.ย. 2016 หรือ การเจาะระบบธนาคารกลางของบังกลาเทศ เมื่อ ก.พ. 2559
- “ความเสี่ยงภัยคุกคามทางไซเบอร์” เป็นความเสี่ยงที่ผู้บริหารระดับสูงต้องให้ความสำคัญ องค์กรใหญ่ต่างๆ ควรที่จะต้องเตรียมการรับมือไว้ด้วย

สงครามไซเบอร์ Cyber War

- เป็นการปฏิบัติการเพื่อขัดขวาง ทำลายระบบการข่าวและการสื่อสารของฝ่ายตรงข้าม เพื่อให้ดุลแห่งข่าวสารและความรู้เอียงมาอยู่ฝ่ายเรา
- สงครามไซเบอร์เกิดขึ้นในหลายประเทศทั้งชัดเจน เปิดเผย และซุ่มเงียบ เป็นสงครามเย็นหรือ Cold War เริ่มกลับมาใช้อีกครั้ง หลังจากการแพ้สงครามเวียดนามของสหรัฐอฯ และการล่มสลายของสหภาพโซเวียตรัสเซีย
- ช่วงสงครามอ่าวที่สหรัฐโจมตีอิรักครั้งที่สอง สิ่งที่สหรัฐทำก่อนอื่นคือ ทำลาย เครือข่ายคอมพิวเตอร์ และอิเล็กทรอนิกส์ของอิรักที่ใช้ควบคุมระบบการยิงของอาวุธ
- การสู้รบปัจจุบันต่างฝ่ายหาทางทำลายระบบคอมพิวเตอร์และอิเล็กทรอนิกส์ที่ควบคุมการยิงอาวุธก่อน
- องค์การอวกาศ NASA = National Aeronautics and Space Administration ในปี 2554 เคยถูกโจมตีอย่างน้อย 10 ครั้ง ทั้งๆที่ลงทุนป้องกันกว่า 58 ล้านเหรียญ (ประมาณ 1,740 ล้านบาท)

สงครามไซเบอร์ Cyber war

- เมื่อ พฤษภาคม 2007 ประเทศเอสโทเนีย ถูกโจมตีด้วยไซเบอร์อย่างหนักโดยเฉพาะ รัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่าง ๆ จนข้อมูลเสียหายพังยับเยิน
- กันยายน ปี 2007 ติกเพนทากอน กระทรวงกลาโหม สหรัฐอเมริกา และที่ทำการรัฐบาล ของฝรั่งเศส เยอรมัน และอังกฤษ ถูกโจมตีด้วยคอมพิวเตอร์ซึ่งมีต้นกำเนิดจากประเทศจีน ได้รับความเสียหาย อย่างหนัก แต่รัฐบาลจีนได้ปฏิเสธข้อกล่าวหา
- วันที่ 14 ธันวาคม ปี2007 เว็บไซต์ของคณะกรรมการการเลือกตั้งกลางประเทศเกียร์กีซ (Kyrgyz) ถูก โจมตีอย่างหนักระหว่างการเลือกตั้งจนทำให้การเลือกตั้งโกลาหล ซึ่งบนเว็บไซต์ระบุชัดเจนว่า เว็บไซต์นี้ถูกโจมตีโดยองค์กรดรีม (Dream) แห่งเอสโทเนีย

รูปแบบการทำสงครามทางไซเบอร์

การใช้คอมพิวเตอร์และอินเตอร์เน็ตเพื่อการทำสงคราม ปัจจุบันมีอยู่ 8 รูปแบบ คือ

1. การโจรกรรมหรืออาชญากรรมทางไซเบอร์ (Cyber Crime)
2. การทำลายเว็บไซต์ การโจมตีเว็บ หรือบล็อคเว็บ (Web attacks)
3. การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านทางอินเตอร์เน็ต
4. การเจาะข้อมูลและการล้วงความลับข้อมูล
5. การกระจายเพื่อให้ปฏิเสธหรือหยุดบริการ (Distributed Denial-of-Service หรือ DDoS attacks)
6. การรบกวนเครื่องมือและอุปกรณ์ที่ใช้คอมพิวเตอร์ควบคุมการทำงาน
7. การโจมตีโครงสร้างระบบสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) และโครงสร้างพื้นฐานที่สำคัญ เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์
8. การใช้อุปกรณ์คอมพิวเตอร์หลอกแต่ซ่อนซอฟต์แวร์ไวรัสเอาไว้
9. การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน หากระบบคอมพิวเตอร์ถูกทำลาย อาวุธนั้นก็ทำงานไม่ได้หรือทำงานไม่แม่นยำ

การโจมตีทำลายระบบ

- เมื่อมีพาณิชย์อิเล็กทรอนิกส์มากขึ้นก็มีอาชญากรรมไซเบอร์ (e-crime) เพิ่มขึ้นเป็นเงาตามตัว
- ปี 2554 ยอดเงินอาชญากรรมไซเบอร์สูงถึง 338 พันล้านเหรียญ(ประมาณ 10 ล้านล้านบาท)
- เชื่อกันว่ายอดความเสียหายจากสงครามไซเบอร์จะมากกว่าความเสียหายในพาณิย์อิเล็กทรอนิกส์มากมายหลายเท่า
- ในสงครามไซเบอร์นั้น แทนที่จะใช้กำลังทางกายภาพก็ใช้ซอฟต์แวร์ในการทำลาย:
  - ระบบโทรคมนาคม (Telecommunication)
  - ระบบส่งกำลังไฟฟ้า (Power Grid)
  - โรงกลั่นน้ำมัน (Petro Plant)
  - โรงไฟฟ้านิวเคลียร์ (Nuclear Power Plant)
  - ระบบท่อส่งแก๊ส(Gas System)
  - ระบบน้ำประปา (Water System)
  - ระบบท่อน้ำทิ้ง (Sewer System) ฯลฯ

การใช้คอมพิวเตอร์และอินเตอร์เน็ตเพื่อการทำสงคราม

- ปัจจุบันมีอยู่ 8 รูปแบบ คือ
  1. การโจรกรรมทางไซเบอร์
  2. การทำลายเว็บไซต์
  3. การโฆษณาชวนเชื่อทางอินเตอร์เน็ต (เว็บไซต์)
  4. การรวบรวมและการล้วงความลับข้อมูล
  5. การกระจายเพื่อให้ปฏิเสธบริการ
  6. การรบกวนเครื่องมือและอุปกรณ์
  7. การโจมตีโครงสร้างระบบสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) พื้นฐานที่สำคัญ
  8. การใช้อุปกรณ์คอมพิวเตอร์หลอกแต่ซ่อนซอฟต์แวร์ไวรัสเอาไว้

การก่อการร้ายในยุค IT

- การเปลี่ยนแปลงสิ่งต่างๆอย่างต่อเนื่องในปัจจุบัน ทำให้เกิดการเปลี่ยนแปลงวิธีการของการก่อการร้ายเช่นกัน
- มุมมองต่อการก่อการร้ายและการต่อต้านการก่อการร้าย มีความสลับซับซ้อนมากขึ้น มีการเปลี่ยนแปลงไปสู่วิธีคิด รูปแบบ ขั้นตอน และการปฏิบัติการในรูปแบบใหม่ๆ
- หากกองทัพยังคงใช้กรอบแนวคิด หลักนิยม แผนและระเบียบปฏิบัติประจำเดิมๆ ในการเผชิญกับการก่อการร้ายที่เกิดขึ้นจะไม่ดีนัก เพราะจะไม่สามารถยุติหรือเอาชนะกลุ่มก่อการร้ายที่เปลี่ยนรูปแบบ วิธีการ และวิธีคิดไปแล้วได้
- การศึกษาถึงรูปแบบการก่อการร้ายในยุค IT จึงมีความจำเป็นที่กองทัพ และส่วนงานที่เกี่ยวข้อง และผู้ที่สนใจจะต้องทำความเข้าใจ เพื่อที่จะได้มีความเข้าใจสภาวะภัยคุกคามและปัญหาที่มาจากภัยก่อการร้ายในปัจจุบันได้ดียิ่งขึ้น

เรากำลังเข้าสู่ยุคสงครามที่ไม่รู้ว่าใครเป็นผู้ก่อการร้ายกันแน่

หน่วยงานความมั่นคงทั่วโลกเปลี่ยน mindset

- ปรับโครงสร้างและวิธีคิด มุ่งเน้นการสร้างความร่วมมือระหว่างประเทศทั้งกับภาครัฐและภาคเอกชน
- การประสานงาน และร่วมมือแลกเปลี่ยนข้อมูลกับบริษัทเอกชน เช่น Google, Facebook, Youtube โดยส่งเจ้าหน้าที่และผู้บริหารระดับสูงไปเข้าร่วม Cybersecurity forum ต่างๆ จนถึงงานประชุมในทุกระดับ
- Best practices ในหลายประเทศพบว่า เข้าร่วมในฐานะ Partnership จะทำให้เกิดความร่วมมือและช่วยเหลือจากบริษัทเหล่านั้นในเชิงลึก เพื่อช่วยสกัดกั้น content ที่เป็นภัยต่อความมั่นคง ไปจนถึงการให้ข้อมูลเชิงลึกต่อการติดตามจับกุมผู้กระทำความผิดได้โดยง่ายอีกด้วย
- Landscape ของความมั่นคงของชาติได้เปลี่ยนไปแล้วในวันนี้ เส้นเขตแดนของประเทศถูกทำลายลงจากความก้าวหน้าของเทคโนโลยี ผู้นำและผู้บริหารทั้งภาครัฐและภาคเอกชนจำเป็นต้องเปลี่ยนวิธีคิด (mindset) โดยต้องร่วมมือกัน และต้องมองขาดว่าสิ่งที่เรากำลังเผชิญไม่สามารถแก้ปัญหาด้วยวิธีคิดเดิมๆ ได้อีกต่อไป

หน่วยบัญชาการไซเบอร์ (Cyber Command)

- หน่วยบัญชาการไซเบอร์สหรัฐมีการรวมทั้ง 3 เหล่าทัพขึ้นตรงต่อ รมว.กห.สหรัฐฯ
- ประเทศกว่า 20 ประเทศมีการจัดตั้งหน่วยดังกล่าว มีทั้งเล็กใหญ่ตามรูปแบบของแต่ละประเทศ หากเราไม่มี Cyber Command จะไม่มีใครสนใจด้านไซเบอร์
- ประเทศไทยต้องออกแบบการพัฒนาไซเบอร์ และมองให้ออกว่ามันได้ประโยชน์ต่อประเทศอย่างไร ต้องหาผู้เชี่ยวชาญ รวมคนเหล่านั้นเข้าด้วยกัน
- กรณี 9/11 เราให้ความสำคัญหน่วยงานที่เป็นโครงสร้างพื้นฐาน สร้าง Red Team เพื่อการซักซ้อมแผนเผชิญเหตุ ซักซ้อมการโจมตี การวางแผนสำรองกรณีฉุกเฉิน ให้กระทรวงทั้งหมดปรับการทำงาน โดยไม่ต้องมีการสั่งการจากศูนย์บัญชาการเพียงอย่างเดียว แม้จะมีศูนย์บัญชาการสำรองอาจจะไม่มีคนเพียงพอ ก็ต้องพยายามเฝ้าระวังในทุกๆวันอย่างต่อเนื่อง
- การฝึกด้านไซเบอร์ต้องทำบ่อยๆ แผนในเอกสารไม่มีประโยชน์ จะต้องทำจริง ปฏิบัติจริง เรื่องอาชญากรรมข้ามชาติต้องมีความร่วมมือในการติดตามจับกุมและมีมาตรการลงโทษประเทศที่ไม่ให้ความร่วมมือ

สถิติการละเมิดข้อมูล

- มี App มือถือที่เป็นอันตรายราว 24,000 รายการ ที่ถูกบล็อกทุกวัน (Symantec)

- ผลจากการศึกษาของสถาบัน Ponemon ในปี 2017 จำนวนที่ถูกละเมิดข้อมูลที่ถูกบันทึกตามประเทศต่างๆ เฉลี่ยแล้วมี 24,089 ครั้ง มากที่สุดต่อปี คืออินเดียที่มีไฟล์มากกว่า 33k ไฟล์ สหรัฐอเมริกามี 28.5k

Source: www.varonis.com/blog/cybersecurity-statistics/

การโจมตีระบบธนาคาร 5 แห่งในรัสเซีย เมื่อ 8 พ.ย 2559

- ธนาคาร 5 รายใหญ่ในรัสเซีย ได้แก่ **ธนาคาร** Sberbank, Alfa Bank, Bank of Moscow, Rosbank และ Moscow Exchange มีเครื่องคอมพิวเตอร์และอุปกรณ์ IoT กว่า 24,000 เครื่อง
- ถูกโจมตีอุปกรณ์ในรูปแบบของ distributed-denial-of-service (DDoS) ซึ่งเป็นการส่งคำสั่งไปยัง Server จำนวนล้านครั้ง เพื่อทำให้ระบบทั้งหมดเข้าสู่สถานะ Offline แล้วแฮ็คเกอร์ก็ทำการขโมยข้อมูล
- ธนาคารต้องใช้เวลาถึง 2 วันในการทำให้ระบบกลับสู่สภาพปกติ แต่เนื่องจากธนาคารจากรัสเซียได้มีการเตรียมพร้อมสำหรับการโจมตีที่ดีอยู่แล้ว จึงสามารถรับมือกับการโจมตีครั้งนี้ได้ และยังคงให้บริการผู้ใช้งานได้อย่างต่อเนื่อง
- ธนาคาร Sberbank แห่งรัสเซียที่ตกเป็นหนึ่งในเหยื่อการโจมตีครั้งนี้ ก่อนหน้านี้ก็เคยถูกกโจมตี DDoS มาก่อนแล้ว 68 ครั้ง ภายในปีนี้ปีเดียว
- การโจมตีครั้งนี้เกินกว่าครึ่งมาจาก ประเทศสหรัฐอเมริกา อินเดีย ไต้หวัน และอิสราเอล

การเจาะระบบธนาคารกลางของบังกลาเทศ

- **ลักษณะการก่อการร้าย :** แฮกเกอร์เจาะระบบ SWIFT (Society for Worldwide Interbank Financial Telecommunication) เป็นระบบเครือข่ายที่ใช้สื่อสาร โดยใช้ Malware โจมตีระบบด้านการเงินระหว่างธนาคารผ่านระบบคอมพิวเตอร์ที่ใช้ในธนาคารทั่วโลก
- **ความเสียหาย :** มีการโจรกรรมหรือถ่ายโอนเงินทุนสำรองไปยังศรีลังกาและฟิลิปปินส์ ทำให้เกิดความเสียหายมูลค่ากว่า 3 หมื่นล้านบาท

- **มัลแวร์(Malware)** คือ ไวรัสตัวหนึ่งที่ถูกปล่อยลงไปในระบบ เพื่อให้ระบบรวนและเสียหาย หลังจากนั้น กลุ่มคนร้ายก็ใช้ระบบใหม่ที่ตัวเองเตรียมมาใส่ครอบระบบที่เสียหายดังกล่าวเข้าไป เพื่อสามารถสั่งการ และซ่อนหลักฐาน และหลบเลี่ยงการถูกตรวจจับ

การเจาะระบบธนาคารกลางของบังกลาเทศ

สาเหตุ :

- จากการสอบสวนพบว่า มาจากการใช้อุปกรณ์รักษาความปลอดภัยราคาถูก และ Firewalls ไม่ได้ทำงานเต็มประสิทธิภาพ เนื่องจากติดปัญหาด้าน License
- ทางเจ้าหน้าที่ไม่ทำการติดตั้งระบบป้องกัน Firewalls ระหว่างระบบ RTGS และระบบ SWIFT เพื่อป้องกันการโจมตีจาก Malware เถื่อน
- ผู้ที่ทำการติดตั้งสวิชระบบเพื่อควบคุมการเชื่อมต่อเข้าสู่ระบบ SWIFT เจ้าหน้าที่เหล่านี้กลับเลือกใช้วิธีการที่ล้าสมัย ซึ่งไม่เคยใช้ในระบบธนาคาร มากกว่าที่จะเลือกใช้วิธีการที่มีความปลอดภัยสูงและล้ำสมัยเพื่อทำให้ทางธนาคารสามารถควบคุมการผ่านเข้าสู่ระบบ
- นอกจากนี้ยังพบว่าคนในมีส่วนเกี่ยวข้องด้วยจึงอาจเป็นเหตุผลหนึ่งที่ทำให้ระบบมีช่องโหว่จำนวนมากที่ทำให้ระบบคอมพิวเตอร์ของธนาคารกลางบังกลาเทศตกอยู่ในความเสี่ยง

การเจาะระบบธนาคารกลางของบังกลาเทศ

แนวทางการป้องกัน :

- หมั่นดำเนินการตามกระบวนการตรวจสอบความปลอดภัยของระบบ เพื่อตรวจสอบว่ามีช่องโหว่ทางด้านความปลอดภัยหรือไม่ เพื่อเร่งปิดช่องโหว่เหล่านั้น รวมทั้งตรวจสอบการทำงานของพนักงานภายในที่ดูแลระบบความปลอดภัยนี้ด้วย
- หมั่นตรวจสอบความเป็นไปรอบตัวทั้งในและนอกองค์กร
- ธนาคารควรแลกเปลี่ยนข้อมูลความเคลื่อนไหวของกลุ่มแฮกเกอร์ให้เป็นที่รับทราบระหว่างกัน
- ทำให้ระบบเป็นเอกเทศ โดยการติดตั้งระบบให้อยู่ในระบบ LAN เพื่อให้ไม่สามารถเชื่อมต่อเข้ากับระบบเครือข่ายคอมพิวเตอร์ส่วนกลางของทางธนาคารกลาง หรือไม่สามารถเข้าระบบจากภายนอกผ่านทางอินเตอร์เน็ตได้
- การใช้รหัสผ่านที่คาดเดาได้ง่าย
- เทคโนโลยีด้านความปลอดภัยนั้นไม่ใช่แค่การติดตั้งซอฟต์แวร์ หรือฮาร์ดแวร์ แต่ต้องเกิดจากการทำงานร่วมกัน ทั้งคนและเครื่องจักร รวมถึงระบบการทำงาน ความปลอดภัยของเครือข่ายจึงจะเกิดขึ้นได้จริง

การเจาะระบบเครื่อง ATM ของธนาคารออมสิน

- **ลักษณะการก่อการร้าย :**
- เมื่อวันที่ 23 ส.ค. 2559 แฮกเกอร์ได้เจาะระบบเครื่อง ATM ของธนาคารออมสิน อาศัยช่องโหว่ของซอฟต์แวร์ภายในตู้ ATM โดยใช้โปรแกรม Malware เข้าไปหลอกเครื่องว่ากำลังมีคนกดเงิน และทำให้เครื่อง ATM รวม 21 ตู้ปล่อยเงินออกมา โดยพบว่าเป็นการโจรกรรมเงินเฉพาะเครื่อง ATM ที่ติดตั้งนอกสถานที่ (Stand Alone)
- **ความเสียหาย :** เงินที่ถูกโจรกรรมไปรวมกว่า 12 ล้านบาท

ประเทศต่าง ๆที่มีนัก Hacker ปฏิบัติงานมากน้อยตามลำดับดังนี้

1.ประเทศจีน เป็นประเทศที่มีแฮกเกอร์มากที่สุดในโลก มีหลายกลุ่มและมีการตั้งเป็นองค์กร ท้าทายรัฐบาลที่ลิดรอนเสรีภาพ ฝ่ายกองทัพเองก็มีสายสัมพันธ์กับบางกลุ่ม โดยดึงเข้ามาร่วมงาน มอบภารกิจให้โจมตีไซเบอร์ที่รัฐบาลเห็นว่าเป็นภัยความมั่นคงของประเทศ

2.ประเทศอเมริกา เป็นมหาอำนาจที่สามารถเจาะข้อมูลได้อย่างชำชอง แฮกเกอร์มีหลายกลุ่มและมีอิทธิพลสูงมาก อย่างกลุ่ม MOD, LOD ซึ่งบรรดาเหล่าแฮกเกอร์นี้ถือเป็นกลุ่มที่มีความสามารถในการเจาะข้อมูลต่างๆได้อย่างขั้นเทพ

3.ประเทศรัสเซีย เป็นประเทศที่ให้บรรดาเหล่าแฮกเกอร์มีอำนาจในการแฮกข้อมูลประเทศต่างๆ และแฮกเกอร์ส่วนใหญ่ก็เป็นแฮกเกอร์ที่สร้างความเสียหายได้ระดับโลก โดยบริษัทยักษ์ใหญ่อย่าง Microsoft, Apple พวกนี้มักจะโดนแฮกเกอร์รัสเซียท้าทายอยู่บ่อยครั้ง

4.ประเทศตุรกี ตุรกีเป็นประเทศที่มีแฮกเกอร์ที่มีความชำนาญสูง มีการตั้งกลุ่มทำงานกันเป็นทีม จะทำการแฮกเว็บไซด์เป็นจำนวนมาก ซึ่งกลุ่มมักจะกล่าวอ้างอยู่เสมอว่า สิ่งที่พวกเขาทำก็เพื่อสันติภาพและยุติสงครามอันเลวร้าย

5.ประเทศบราซิล บราซิลเป็นศูนย์กลางของบรรดาเหล่านักแฮกเกอร์ที่ชอบแฮกข้อมูลทั้งในทวีปเอเชียและยุโรป ประชากรส่วนใหญ่ของประเทศ**มักจะชอบทำธุรกรรมทางการเงินผ่านระบบออนไลน์** จึงเป็นจังหวะดีที่แฮกเกอร์ขโมยเงินในบัญชีทางอินเตอร์เน็ต ซึ่งมีข่าวให้เห็นอยู่บ่อยครั้ง

ประเทศต่าง ๆที่มีนัก Hacker ปฏิบัติงานมากน้อยตามลำดับดังนี้

6.ไต้หวัน เป็นประเทศอิสระ แต่จีนถือว่าเป็นมลฑลหนึ่งเท่านั้น ปัญหาทางการเมืองทำให้แฮกเกอร์โจมตีอยู่ต่อเนื่อง ซึ่งระบบอินเตอร์เน็ตของไต้หวันถือเป็นศูนย์กลางที่มักจะโดนพวกมัลแวร์โจมตีอยู่บ่อยๆ

7.ประเทศอินเดีย เป็นประเทศผู้นำทางด้านไอทีและคอมพิวเตอร์ จึงมีแฮกเกอร์เก่งๆอยู่เป็นจำนวนมาก ซึ่งแฮกเกอร์ส่วนมากเป็นนักรณรงค์ต่อต้านเรื่องต่างๆ จากการแฮกและพยายามท้าทายระบบเซ็นเซอร์อินเตอร์เน็ต

8.ประเทศโรมาเนีย เป็นประเทศที่มีขนาดเล็ก แต่มีแฮกเกอร์เก่งๆจำนวนมาก ที่อยู่ของแฮกเกอร์จะอยู่ในเมืองขนาดเล็ก ซึ่งถือเป็นสถานที่ที่ปลอดภัยและเป็นสวรรค์ในการกบดานของบรรดาเหล่านักอาชญากร

9.ประเทศฮังการี เป็นประเทศเล็ก แต่ก็มีการโจมตีจากเหล่าแฮกเกอร์มาก ประเทศในแถบยุโรปจะมีการป้องกันการโจมตีของเหล่าแฮกเกอร์เอาไว้เป็นอย่างดี แต่สำหรับประเทศฮังการีเป็นประเทศที่ตกเป็นเป้าหมายจากบรรดาเหล่าแฮกเกอร์ให้ทดสอบอยู่เสมอ

10.ประเทศอิตาลี มักจะโดนโจมตีจากกลุ่มไซเบอร์อยู่บ่อยครั้ง คิดแล้วประมาณ 1.6 เปอร์เซ็นต์เมื่อเทียบกับประชากรทั้งโลก โดยมีเหล่าแฮกเกอร์ที่มีชื่อเสียงได้ทำการแฮกเว็บไซต์ของรัฐบาลและก็เจาะข้อมูล

การจัดอันดับ Global Cybersecurity Index (GCI) 2017

- 10 อันดับประเทศที่ได้คะแนนสูงสุด จากทั้งหมด 164 ประเทศทั่วโลก ได้แก่

อันดับ	ประเทศ
1	สิงคโปร์
2	สหรัฐอเมริกา
3	มาเลเซีย
4	โอมาน
5	เอสโตเนีย
6	มอริเชียส
7	ออสเตรเลีย
8	จอร์เจีย และ ฝรั่งเศส
9	แคนาดา
10	รัสเซีย

Global Cybersecurity Index ranking 2017

Country	GCI score*	2017 ranking	2015 ranking
Singapore	**0.92**	**1**	**6**
United States	0.91	2	1
Malaysia	0.89	3	3
Oman	0.87	4	3
Estonia	0.84	5	5
Mauritius	0.82	6	9
Australia	0.82	7	3
Georgia	0.81	8	12
France	0.81	9	9
Canada	0.81	10	2

*Normalised

Source: U.N. INTERNATIONAL TELECOMMUNICATION UNION
STRAITS TIMES GRAPHICS

- หน่วยงาน National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา ทำหน้าที่กำหนดมาตรฐานเทคโนโลยีสารสนเทศ ได้วางแนวทางการรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity framework) เพื่อให้หน่วยงานของภาครัฐ เอกชน รวมถึงสถาบันการเงินต่างๆ ใช้เป็นแนวทางในการปฏิบัติ
- ธนาคารกลางของอังกฤษ สหรัฐอเมริกา และสิงคโปร์ ได้จัดให้มีการทดสอบการรับมือ Cyber Attack ในระดับประเทศมาตั้งแต่ปี 2554

Thank you

www.facebook.com/ekkachai.srivilas
www.elifesara.com